

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 01-180656

(43)Date of publication of application : 18.07.1989

(51)Int.Cl.

G06F 12/16

(21)Application number : 63-004599

(71)Applicant : FUJI ELECTRIC CO LTD

(22)Date of filing : 12.01.1988

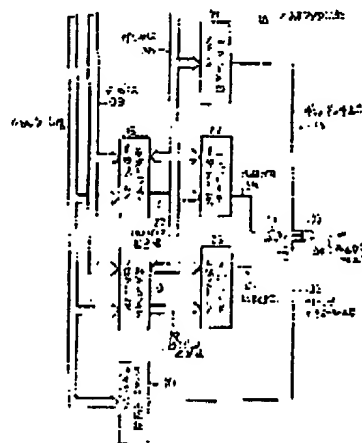
(72)Inventor : KOMINE SHIGERU

(54) MEMORY PROTECTING DEVICE

(57)Abstract

PURPOSE: To protect the memory area of another task by inhibiting a writing into the memory area except a writable area specified by a lower limit and an upper limit address setting registers, rewriting dynamically the values of both the registers by an OS at the time of switching the task and making only the area of the task being executed into the writable area.

CONSTITUTION: A lower limit address setting register 18 and an upper limit address setting registers 19 to set the writing inhibiting area are provided and the writing into the writing inhibiting area is detected by comparing addresses outputted from both the registers 18 and 19 and a CPU by a lower limit address comparator 22 and an upper address comparator 23. The contents of the lower limit and the upper limit address setting registers 18 and 19, that is, the writing inhibiting area is changed dynamically for every task by an operating system. Thus, a certain task is prevented from executing a wrong writing into the memory area or the I/O area of another task.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

⑨ 日本国特許庁(JP) ⑩ 特許出願公開
 ⑪ 公開特許公報(A) 平1-180656

⑫ Int. Cl.⁴
 G 06 F 12/16

識別記号
 310

庁内整理番号
 H-7737-5B

⑬ 公開 平成1年(1989)7月18日

審査請求 未請求 請求項の数 1 (全6頁)

⑭ 発明の名称 メモリ保護装置

⑮ 特 願 昭63-4599

⑯ 出 願 昭63(1988)1月12日

⑰ 発 明 者 小 峯 繁

神奈川県川崎市川崎区田辺新田1番1号 富士電機株式会社内

⑱ 出 願 人 富士電機株式会社

神奈川県川崎市川崎区田辺新田1番1号

⑲ 代 理 人 弁理士 山口 巖

明 細 書

1. 発明の名称 メモリ保護装置

2. 特許請求の範囲

1) オペレーティング・システムによりマルチタスク処理を行い、かつ前記タスクはこのオペレーティング・システムを介して1/0アクセスを行うように構成された電子計算機システムにおいて、

前記マルチタスク処理の開始時点、処理対象タスクの切換え時点、または処理中のタスクの1/0アクセス時点において、前記オペレーティング・システムによって設定されるアドレス値であって、現に実行しようとするタスク、またはアクセスしようとする1/0についてのアドレスの上限値および下限値(以下それぞれ上限アドレス設定値および下限アドレス設定値という)をそれぞれ設定される上限アドレス設定レジスタおよび下限アドレス設定レジスタと、

アドレスバス上に出力されるアドレス値が、前記上限アドレス設定レジスタおよび下限アドレス設定レジスタをそれぞれアクセスするアドレス値

で無く、かつ前記上限アドレス設定値または下限アドレス設定値のいずれかを越えるものであり、さらにこのとき同時に制御バス上に書込信号が出力されていることを検出して異常警報信号を出力する不正書込検出手段と、を備えたことを特徴とするメモリ保護装置。

3. 発明の詳細な説明

【産業上の利用分野】

この発明は電子計算機のメモリ保護装置、特にメモリ管理機構を持たないマイクロプロセッサをCPUとし、マルチタスク処理(即ち複数タスクの並列処理)を行う電子計算機のメモリ保護装置に関する。

なお以下各図において同一の符号は同一もしくは相当部分を示す。また論理もしくはレベルHigh、Lowは単にH、Lと記すものとする。

【従来の技術】

メモリ管理機構を持たないマイクロプロセッサをCPUとして用いた電子計算機においては、プログラムの誤り(バグ)等によりCPUが暴走し

特開平1-180656 (2)

た場合、あるいはプログラムの誤りそのものにより、不正なアドレスに対してデータの書き込みをしてしまうことがある。このような場合、プログラムが破壊されたりI/O機器が異常動作したりしてしまう。

このような不正な書き込みに対してメモリを保護する方法として、メモリ空間を書込み可能な領域と書き込み不可能な領域とに予め設定しておき、書き込み不可能な領域に書き込みが行われた場合に、ハードウェア的にこの不正な書き込みを検出し、割込みによりCPUに知らせるという方法がある。

例えば第3図のようなメモリマップを持つ電子計算機においてRAM領域1およびI/O領域3は書き込み可能であり、未実装領域2およびROM領域4は書き込み禁止であるとする。

このような場合、書き込み禁止領域への書き込み動作を検出するために、第4図例のようにアドレスバスABの上位値の一部の信号線6と、書き込み信号7とをアドレスデコード回路8によってデコードし、不正なアドレスに対する書き込みに対して割込

出力9に有効にし、図外のCPUに割込みをかけるという方法が知られている。また第4図例のようにアドレスデコード回路8と同等の回路としてROM10等を用いる方法もある。

【発明が解決しようとする問題点】

しかしながら、前記の方法は書き込み可能領域としてのI/O領域3に対して何も保護がなされていないため、例えばプリンタ装置に異常なデータが出力されてしまうことを防ぐことができないという問題点がある。

また、マルチタスク処理を行うシステムにおいては、RAM領域1に複数のプログラム(タスク)が同時に存在するが、従来の方法では各タスクのメモリ領域は全て書き込み可能であるため、あるタスクが他のタスクのメモリ領域に対して不当な書き込みを行うのを防ぐことができないという問題点が存在する。

そこで本発明の目的は、I/O領域への不正な書き込みを防ぐことができ、しかもマルチタスク処理においてあるタスクの他のタスクのメモリ領域

に対する不正な書き込みを防ぐことができる手段を備えたメモリ保護装置を提供することにある。

【問題点を解決するための手段】

前記の目的を達成するために本発明の装置は「オペレーティング・システムによりマルチタスク処理を行い、かつ前記タスクはこのオペレーティング・システムを介してI/Oアクセスを行うように構成された電子計算機システムにおいて、

前記マルチタスク処理の開始時点、処理対象タスクの切換え時点、または処理中のタスクのI/Oアクセス時点において、前記オペレーティング・システムによって設定されるアドレス値であって、現在実行しようとするタスク、またはアクセスしようとするI/Oについてのアドレスの上限値および下限値(以下それぞれ上限アドレス設定値(28など)および下限アドレス設定値(27など)という)をそれぞれ設定される上限アドレス設定レジスタ(19など)および下限アドレス設定レジスタ(18など)と、

アドレスバス(ABなど)上に出力されるアド

レス値が、前記上限アドレス設定値レジスタおよび下限アドレス設定値レジスタをそれぞれアクセスするアドレス値で無く、かつ前記上限アドレス設定値または下限アドレス設定値のいずれかを越えるものであり、さらにこのとき同時に制御バス上に書き込み信号が出力されていることを検出して異常警報信号(不正書き込み出力91など)を出力する不正書き込み検出手段(アドレスデコード回路21、下限アドレスコンパレータ22、上限アドレスコンパレータ23、ORゲート31、タイミングコントロール回路20、ANDゲート35など)と、を備えた」とものとする。

【作用】

この発明は、書き込み禁止領域を設定するための下限アドレス設定レジスタと上限アドレス設定レジスタとを設け、前記両レジスタとCPUより出力されるアドレスとを下限アドレスコンパレータおよび上限アドレスコンパレータによって比較することにより書き込み禁止領域への書き込みを検出し、前記下限および上限アドレス設定レジスタの内容、

特開平1-180656(3)

すなわち書き込み禁止領域を、OS（オペレーティング・システム）によってタスクごとに動的に変更することによって、あるタスクが他のタスクのメモリ領域やI/O領域に対して不正な書き込みを行うのを防ぐようにしたものである。

【実施例】

第2図は本発明による電子計算機の構成を示す。同図においてCPU部11はマイクロプロセッサおよびクロックジェネレータ、バスコントローラ、バスバッファ等の周辺回路からなり、この部分11はメモリ管理機構を持っていない。CPU部11よりアドレスバスAB、データバスDB、制御バスCBからなる主バスMBを介して、メモリ部12、I/O部13、不正書き込み検出部14が接続されている。メモリ部12はRAM、ROM、制御回路等から成り、I/O部13はI/O制御回路等から成る。I/O部13はI/Oバス17を介してI/O装置15と接続されている。

次に不正書き込み検出部14の構成を第1図に示す。マルチタスク処理を行う電子計算機システムにお

いては、OS（オペレーティング・システム）がタスク管理やI/O管理等を全て行う。アプリケーション・プログラム、従ってタスクからはI/O装置との直接のやりとりは行わず、OSにI/O装置15とのやりとりを依頼する。

マルチタスク用OSは各タスクの実行状況を記憶しておく領域を持っている。この記憶領域は通常TCB（Task Control Block）と呼ばれ、各々のタスクが実行中中断された場合のレジスタ値などが格納されている。

本発明においては各タスクごとに、そのタスクのメモリ領域の下限（最低位）アドレスと上限（最高位）アドレスとを考える。各タスクごとの下限アドレス、上限アドレスが実際に決定するのは、OSが補助記憶装置（ハードディスク、フロッピーディスク等）からプログラム（ロードモジュール）をロードするときであるが、この際にOSは各タスクごとのTCBの中に、そのタスクのメモリ領域の下限アドレスと上限アドレスとを格納するものとする。

OSは各タスク切換え時に、現在実行中のタスク（タスク1とする）のレジスタ値をタスク1のTCB（TCB1）に格納し、これから実行しようとするタスク（タスク2）のレジスタ値をタスク2のTCB（TCB2）よりロードする。さらにTCB2中のタスク2の下限アドレスを下限アドレス設定レジスタ18に設定し、タスク2の上限アドレスを上限アドレス設定レジスタ19に設定する。このようにして下限アドレス設定レジスタ18、上限アドレス設定レジスタ19には、それぞれ現在実行中のタスクの下限アドレス、上限アドレスが設定されることになる。

そしてCPUが現在、アドレスバスABに出力しているアドレスと、下限アドレス設定レジスタ18への設定値27とを下限アドレスコンパレータ22により、また同じく前記アドレスと上限アドレス設定レジスタ19への設定値28とを上限アドレスコンパレータ23により、それぞれ比較する。

従ってもしCPUが現在実行中のタスクのアドレス領域より低位のアドレスにアクセスした場合、

すなわち下限アドレス設定値27よりアドレスバスABに出力されているアドレス値が小さい場合には下限アドレスコンパレータ22の比較出力29はHレベルになり、この比較出力29を入力信号とするORゲート31の出力32もHレベルになる。同様にCPUが現在実行中のタスクのアドレス領域より高位のアドレスにアクセスした場合、すなわち上限アドレス設定値28よりアドレスバスABに出力されているアドレス値が大きい場合にも上限アドレスコンパレータ23の比較出力30はHレベルになり、この比較出力30をも入力信号とする前記ORゲート31の出力もHレベルになる。

つまりORゲート31の出力32は、上限および下限アドレス設定レジスタ18、19により定められる、現在実行中のタスクのメモリ領域以外のアドレスをCPUがアドレスバスABに出力した場合にHレベルになる。

しかしCPUは常に有効なアドレスをアドレスバスABに出力しているわけではなく、あるアドレスから別のアドレスに切換わる場合や、バスア

特開平1-180656(4)

クセスを行わない場合などにアドレスバスA Bに出力されるアドレスは不定となる。

またタスク切換えは割込みによりタスクからOSに制御が移ることによりOSによって行われる。従ってこのとき割込みベクタ領域やOSの命令コード領域のアドレスがアドレスバスA B上に出力されるが、このこのアドレスは不当なアドレスとしなければならない。つまり、あるタスクの領域以外書き込みは禁止するが、読出しは自由に行えるものとする。読出しによりメモリ内容が破壊されることはないで、メモリ保護のためには書き込みのみ禁止すればよい。

そこでタイミングコントロール回路20は、CPUが書き込み動作を行う場合で、しかもアドレスが確実に有効であるタイミングでのみその出力信号(タイミングコントロール信号)33がHレベルになるようにする。これによってアドレスが不定の期間や、読出し動作の場合に誤った割込信号としての不正書き込出力9AがANDゲート35からCPUに入るのを防ぐ。

両レジスタに書き込みを行うことができない。従って下限および上限アドレス設定レジスタ18、19へは両レジスタのアドレス値にかかわらず、すなわち現在の書き込み可能領域にかかわらず、常に書き込み可能でなければならない。そこで常にこの両レジスタ18、19への書き込みを可能とするのがアドレスデコード回路21で、その出力信号(アドレスデコード信号)34はアドレスバスA Bの値が下限または上限アドレス設定レジスタ18、19をアクセスするアドレス値である場合のみLレベルとなり、それ以外の場合はHレベルとなる。これにより下限または上限アドレス設定レジスタ18、19へのアドレス設定値27または28の書き込みの際は、不正書き込検出部14の検出出力、つまりANDゲート35からの不正書き込出力9Aが有効にならず、両レジスタ18、19へは常に書き込み可能となる。

以上よりCPUがアドレスバスA Bに出力するアドレスが、下限および上限アドレス設定レジスタ18、19により規定される書き込み可能な領域にあるか、または下限、上限アドレス設定レジスタ18、

先に述べたようにマルチタスクシステムではI/OアクセスはOSを通して行われる。特に本方式においてはアプリケーションプログラムがI/O領域に直接書き込みを行うことは不可能であるようにする。なぜならI/Oのアドレスはタスクのアドレス領域の外側にあり、タスクのアドレス領域のみが書き込み可能な領域であるからである。アプリケーションプログラムはI/Oアクセスを行う場合、割込みまたはC A L L命令によってOSに制御を移す。このとき割込みベクタやOSの命令コード領域は書き込み禁止ではあるが、読出しは可能であるのでOSに制御を移しOSの命令コードをCPUが実行することが可能である。OSは上限および下限アドレス設定レジスタ18、19に値を設定し直し、I/Oアドレス領域に書き込むことが可能ないようにしてからI/Oアドレスへのアクセスを行う。

ところが上限および下限アドレス設定レジスタ18、19をアクセスするためのアドレス値もI/Oアドレスに割付けられているので、このままでは

19への書き込みのための(つまり該レジスタ18、19をアクセスする)アドレスであるかでないか、不正書き込検出出力9AはHレベルとなる。この出力9AをCPU割込信号として入力することにより、CPUは不正な書き込みを検知できる。

なお、下限、上限アドレス設定レジスタ18、19へは常に書き込み可能であるが、不正な書き込みにより偶然これらのレジスタに何らかの値を書込み、しかも次のどこかのアドレスに対する書き込みで割込みが起らないという確率は非常に低い。

OSは不正書き込検出出力9AがHレベルとなり、割込みとしてCPUに入力されることによりエラー処理ルーチンに入り、エラーメッセージの出力、異常動作したタスクの実行停止、場合によってはシステム全体の停止等の処理を行う。

【発明の効果】

この発明によれば、下限および上限アドレス設定レジスタによって定まる書き込み可能領域以外のメモリ領域は書き込み禁止とし、OSにより図記両レジスタの値をタスク切換え時に動的に書換え、

特開平1-180656 (5)

実行中のタスクの領域のみを書込み可能領域としたので他のタスクのメモリ領域の保護を行うことができる。

また、I/O領域への書込みはOSのみが行うことができるようにしたので、I/O装置の異常動作を防ぐことができる。

4. 図面の簡単な説明

第1図は本発明の一実施例としての不正書き検出部の構成を示すブロック図、第2図は同じく電子計算機システムの要部構成を示すブロック図、第3図は電子計算機システムのメモリマップ例を示す図、第4図は従来のメモリ保護方式の要部構成を示すブロック図である。

11—CPU部、14—不正書き検出部、18—下限アドレス設定レジスタ、19—上限アドレス設定レジスタ、20—タイミングコントロール回路、21—アドレスデコード回路、22—下限アドレスコンパレータ、23—上限アドレスコンパレータ、31—ORゲート、35—ANDゲート、AB—アドレスバス、DB—データバス、CB—制御バス、9A—不正書き検出力

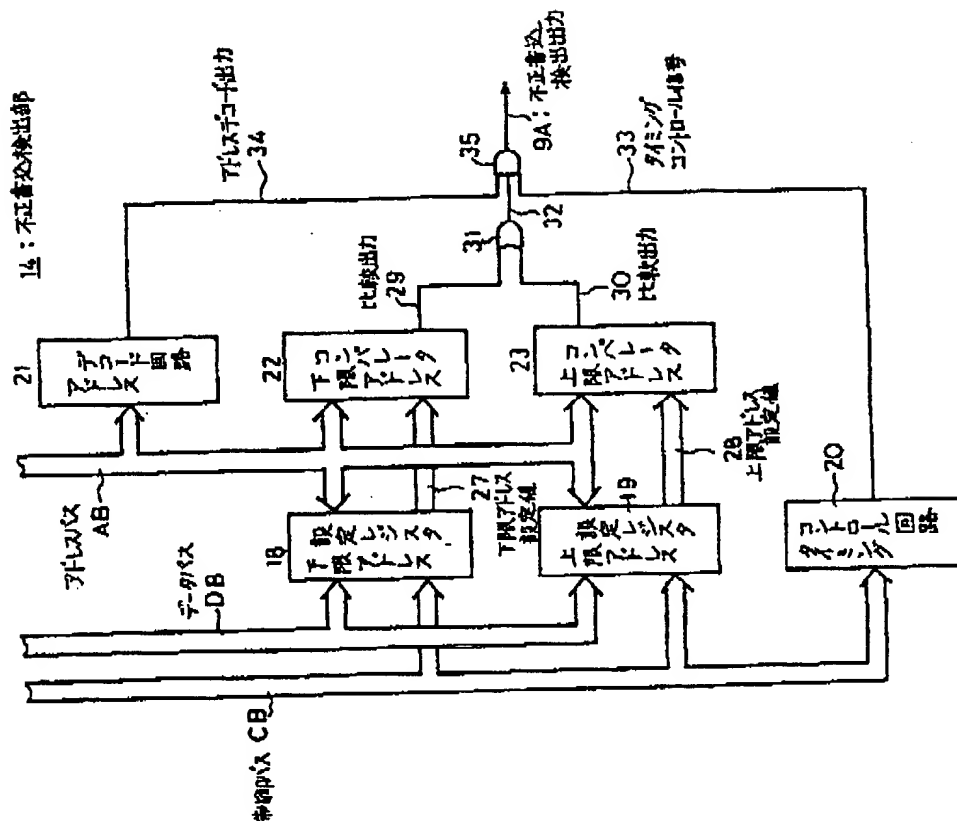


図 1

特開平1-180656(6)

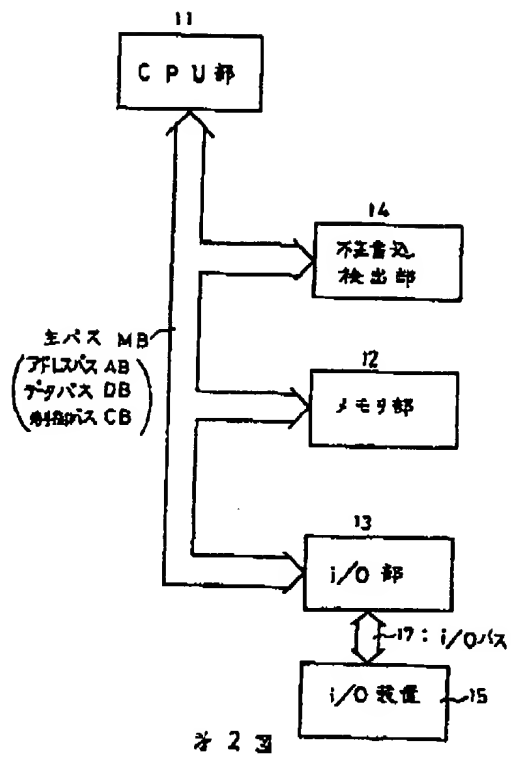


図 2

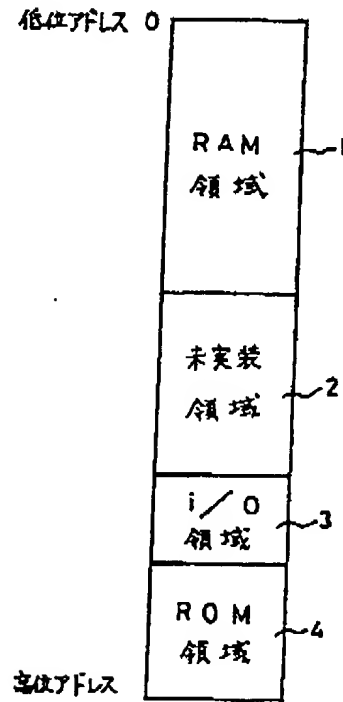
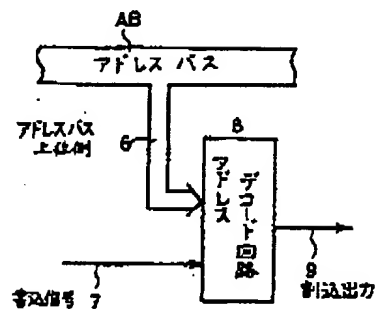
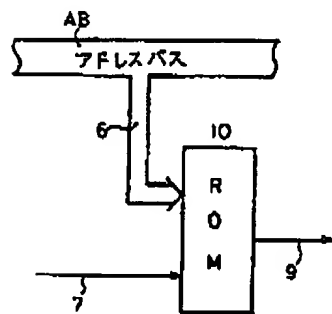


図 3



(a)



(b)

図 4